

## Table of Contents

<b>Section 5: Conducting Assessment .....</b>	<b>2</b>
<b>1. Develop Data Libraries .....</b>	<b>2</b>
Data Libraries .....	2
Performance Testing .....	4
Uncertainties.....	8
<b>2. Path Analysis.....</b>	<b>10</b>
<b>3. Scenario Analysis.....</b>	<b>12</b>
Identify Scenario Sets to Analyze .....	13
Develop Detailed Scenarios .....	14
Review and Select Final Scenarios to Evaluate .....	16
Determine Effectiveness against Scenarios .....	16
Combinations of Nuclear Security Methods and Tools Suggested for Different Conditions.....	17
<b>X: Conducting A Force-on-Force Exercise.....</b>	<b>19</b>

Don't recall how to add Table of Tables:

## Figures

Figure 1. How Scenario Analysis Steps Correspond to the Process for Using Software Tools and Evaluation Methods .....	13
---	----

## **Section 5: Conducting Assessment**

There are three general steps that make up a nuclear security assessment:

1. Develop data Libraries that indicate how effective the physical protection measures are both individually but also as parts of subsystems and actual systems.
2. Perform Path Analysis
3. Perform Scenario Analysis

Depending upon the nature and objectives of the assessment not all three of these steps may need to be performed; for example, at facilities with simple layouts there may not be a need to perform path analysis.

Each of these steps is described below.

### **1. Develop Data Libraries**

#### **Data Libraries**

Data Libraries are a historical collection of performance test data that can be used as a basis to justify nuclear security element probability of detection, assessment, or delay times used in modeling and simulation activities. Data libraries should be developed and maintained as part of any assessment program or process. Data is collected in the initial stages of the assessment process and is essential to the characterization of the facility to provide documented evidence for the facility assessment results. Once established, data libraries can also be used as initial input to other assessments with some confidence that similar nuclear security element configurations will provide comparable detection, assessment and/or delay values for similar installations/configurations. The use of data libraries can also reduce the assessment costs by establishing standard delay, detection and assessment values for use by multiple sites or facilities where common barriers and alarms systems are used. The data libraries can be a manually tabulated list or an electronic menu values embedded in an assessment software program.

Sources where data library values can be derived include the use of state sponsored or other site testing, facility specific performance testing, subject matter expert judgment, and open source data including state law enforcement and military experience. Manufacturer specifications or testing data may be used initially, until other user performance data can be developed.

Data libraries should be protected based upon the highest level of sensitivity of any data contained in the data library.

The assessment will typically start with existing performance testing data and open source information and, if necessary, will collect new data if it is needed during the assessment. The assessment scoping document referred to in section 4 can be used to describe the process and criteria for selecting data library values. Time in the assessment must therefore be allocated to plan for, collect, and document site-specific performance data at the facility.

Annex B describes two techniques for characterizing performance measures such as delay times or detection probabilities: statistical analysis and the use of expert judgement.

Care must be taken in using the data collected during a force-on-force exercise (FoF) and/or a response limited scope performance test (LSPT). The primary purpose of a FoF exercise is to provide assessment of training or insight into overall system effectiveness, not to collect data for use in an assessment. There are also typically practical limitations on the time to conduct the exercise and the safety considerations associated with performing each task that limit the realism of the test or exercise. As an example, expert controllers are needed during exercises to assess the effectiveness of area-kill weapons such as grenades due to safety concerns.

Table 1 provides a list of some of the primary categories of data needed in a data library. As the table indicates, a high degree of dependency exists between the different categories of data. For example, the performance of a barrier cannot be fully determined without knowing the capabilities of the tools that an adversary may use to defeat it. Accounting for this dependency during data collection can speed the process.

**Table 1. SELECTED PERFORMANCE DATA CATEGORIES.**

Category	Typical Parameters	Description
Detectors	Assessment delay and sensor sensitivity	Sensing and assessment data to go with each method of detection (e.g., cameras, eyes).
Tools	Weight, effectiveness, defeat and deploy times	Tools used by adversaries (and protective force) to defeat barriers and objectives.
Weapons	Weight, fire rate, hit and kill probabilities	Weapons used to neutralize adversaries (or protective force) or objectives/targets.
Platforms (people, vehicles)	Speeds over barriers and across terrains	Determines how fast adversaries and responders move on foot or in vehicles.
Barriers	Transparency of barriers to sensors and weapons	Determines how sensors and weapons are impacted by the barriers in a security system.
Terrains	Transparency of terrains to sensors and weapons	Determines how sensors and weapons are impacted by the terrains at a facility.
Humans	Tools, weapons and vehicles assigned	Defines tools, weapons and vehicles assigned to adversaries and responders.

Regardless of the specific methods used to select and reduce the data, it must be retained for quality control purposes. It is recommended to record this information on worksheets even if the modeling and simulation tool has its own interface for capturing data. Typically, the data will need to be reviewed and approved by several organizations, some at the facility and some within the competent authority and it is not reasonable to assume that all of these reviewers have ready access to that tool and the required training on the tool to inspect the database. It is imperative that data collection adhere to quality standards to ensure the confidence given to the accuracy of the data is maintained. The data collection and testing programs should be prioritized to focus on those features that give the greatest benefit to the evaluation.

Once a facility has been adequately characterized during the first assessment, future updates should be more straightforward and can even represent a small incremental cost over the original effort.

### **Performance Testing**

Performance testing by state sponsored testing centers and/or by site resources can be conducted for different types of barriers, sensors, cameras and procedures. Data is based on specific defeat mechanisms associated with barriers, sensors, cameras, procedures, and/or personnel. For example, barrier delay times can be tested for defeat over a range of increasing levels of breaching techniques from hand tools, power tools, breaching tools, explosives, and vehicles, as applicable. Similarly, alarm sensor probability of detection levels are determined for personnel walking, running, jumping, crawling, bridging, and use of other aids, etc.. Typically, multiple iterations of testing can occur on each nuclear security element resulting in a range of test data to ensure a representative sample is collected. Selection of the data library values used for input is then based on either statistical analysis of all test data or professional judgement or a combination of both. Performance testing data can also be derived from state oversight inspections results, routine facility testing organizations, or specific testing as requested by the assessment team to validate critical system element assumptions and input. Performance testing methodologies and results must be **well documented** in order to justify the development or revision of assigned values. The use of video and a full explanation of the performance tests can be very useful to document test data.

**On-site Testing** – Due to unique facility design or environmental conditions that may not match existing library source data, some sites may conduct nuclear security element testing to establish and/or validate assessment input values. If the actual facility is used, detailed coordination is required with facility operations and security to ensure protection measures are maintained during the testing period through compensatory measures. If a deficiency is identified through testing or a protection element is defeated as part of a test (i.e. fence is cut), corrective actions should be initiated as soon as testing is completed. Compensatory measures will remain in place until corrective actions are completed.

**Dedicated Test Bed** – Dedicated test beds can be located at the facility location or as part of a state sponsored testing location. The dedicated test bed approach allows for PPS testing under more realistic conditions without impacting facility operations or security. Due to the wide use of certain PPS elements, a dedicated testing facility may be established to determine and/or validate assessment input values over a wide range of PPS elements, conditions and defeat mechanisms. Any test bed should include facilities to test interior and exterior PPS systems. It should include infrastructure to support sensor testing, data gathering, and data recording. The

test bed should also include the efficient installation of sensor platforms, access control systems, delay systems, contraband detection, lighting, assessment, power distribution, alarm communications, monitoring and recording systems. The test bed can be used for determining performance data for assessments; assess new technologies, training of personnel for operation and maintenance of PP systems. The benefit of using a facility based test bed is that it allows for the testing of facility specific physical protection measures under exact climatic conditions to understand how weather and other site conditions affect sensor performance. This approach also helps to identify the proper calibration and/or installation configuration in order to ensure the optimum system performance.

In some cases, defeat testing of a barrier or alarm system may be prohibited due to cost or operational constraints at a site/facility. These constraints can include attempting to performance test alarm sensors or barriers in areas of high radiation or contamination issues where personnel safety is a concern. In these cases, **subject matter expert judgement** can be relied upon for establishing delay times and/or detection/assessments values. The subject matter experts may perform engineering calculations and/or review historical testing data for similar types of protection elements and assign testing results. If no data exists, subject matter expert opinion and manufacturer specifications/testing values can be the initial basis for assigning values.

**Open source data** comes from various historical test sources or generally accepted information. This information is widely distributed for general use such as ammunition ballistics performance or general explosive characteristics. Other open source information can include manufacturer published or website data for PPS performance, usually under controlled laboratory conditions. Other sources of data may include national **law enforcement or military data and experiences**. For example the use of military handbooks can be a valuable source of information for generic data concerning response tactics, strategies, ballistics and explosive characteristics. An example of such a handbook, that is openly available, is the Swedish “SoldF” [1]. This book contains basic knowledge for all soldiers, regardless if they belong to the army, the marines or the air force. It gives guidance on the soldier’s behaviour, on and outside the battlefield. Specifically there are sections on rules of engagement, on weapon types - including general descriptions on their performance, on armor and on communications. This type of data source, although it is quite general in nature, has the advantage that its quality has been assessed and found to be sufficient as guidance for military personnel. When the information provided is applicable, it may be therefore be expected to be quite realistic.

[1] SoldF – Soldaten i fält (SoldF - Soldier in the field)

There are various reasons to **adjust data library** values. Site specific conditions for barriers or alarm systems may differ from the previous data library tested configurations. Minor design changes in barrier design may dramatically affect standard adversary delay times and defeat methods. Also, advances in both physical protection technologies and adversary defeat

capabilities are also justifications to adjust historical testing data. In other cases, where testing of a barrier or alarm system is possible, data collected by the site/facility on specific adversary scenarios may invalidate existing data library values. Site specific conditions and protection measures can be different than generic testing conditions performed at a state testing location. As a result, site specific testing of both the site protection capabilities (alarm, assessment, response) and the adversary attack methods is always recommended to justify or confirm assessment model inputs.

One method to document **changes or modifications** to standard data library values is for the facility/site to develop an annex to data library that identifies site specific testing results and justifies model inputs in order to properly document assessment inputs for model validation. The benefit of having these test data in a separate annex allows for easy reference and the ability to highlight inputs that deviate from standard historical values.

Tables 2 and 3 provide some brief examples of detection and delay values.

Component Type	Component Description	No Equipment P <sub>D</sub>	Hand Tools P <sub>D</sub>	Power Tools P <sub>D</sub>	High Explosives P <sub>D</sub>	Land Vehicle P <sub>D</sub>
Exterior Sensors	Seismic Buried Cable	0.5	0.5	0.5	0.5	0.9
	Electric field	0.5	0.3	0.3	0.5	0.9
	Infrared	0.8	0.4	0.4	0.5	0.8
	Microwave	0.8	0.7	0.7	0.7	0.9
	Video motion	0.8	0.6	0.6	0.7	0.9
	Multiple non-complementary	0.9	0.8	0.8	0.8	0.99
	Multiple complementary	0.99	0.95	0.95	0.99	0.99
Interior Sensors	Sonic	0.5	0.5	0.5	0.5	N/A
	Capacitance	0.5	0.5	0.5	0.5	N/A
	Video Motion	0.5	0.5	0.5	0.5	N/A
	Infrared	0.5	0.5	0.5	0.5	N/A
	Ultrasonic	0.5	0.5	0.5	0.5	N/A
	Microwave	0.5	0.5	0.5	0.5	N/A
	Multiple non-complementary	0.75	0.75	0.75	0.75	N/A
	Multiple complementary	0.9	0.9	0.9	0.9	N/A
Position Sensors	Position Switch	0.5	0.2	0.2	0.2	N/A
	Balanced Magnetic Switch	0.8	0.8	0.8	0.8	N/A
Fence Sensors	Taut Wire	0.5	0.25	0.25	0.75	0.85
	Vibration	0.5	0.1	0.1	0.75	0.85
	Strain	0.1	0.1	0.1	0.1	0.9
	Electric Field	0.5	0.4	0.4	0.75	0.9
	Multiple Sensors	0.75	0.5	0.5	0.8	0.9

Table 2: Hypothetical Intrusion Detection Sample Data

Barrier Description	Penetration Equipment	Equipment Weight (kg)	Penetration Time (Minutes)			
			Min.	Mean	Max.	Standard Deviation
Sheet Metal Standard industrial pedestrian door, 1.6-mm metal, panic hardware, cylinder lock, rim set, butt hinges with removable pins	Explosives (1.0)	1	1.25	1.9	2.8	
	Cordless drill	2.7	1.5	3.0	4.5	0.61
	Pry bar	7	0.1	0.2	0.3	0.41
	Fire ax	4.5	1.9	3.8	5.7	0.78
	Suction cups, sledge, cutting torch	25	0.5	1.0	1.5	0.20
	Pipe wrench	1	0.2	1.2	2.5	

Table 3: Hypothetical Penetration Times – Door Sample Data

### Types of Performance Testing

A new performance test can be regarded as a scientific experiment; the hypothesis being tested is that the PPS does not resist the threat at an acceptable level, as determined in the test plan. In this fashion test error rates control the probability that the measure(s) under test meet acceptable performance levels against the threat when they actually do not.

### Performance Testing of technical systems

The functionality of technical security systems (detectors, alarms, communications etc.) is mostly a matter for routine monitoring and inspection. However, they may also be performance tested, especially with regard to their inputs to analysis systems and controls requiring a human response.

### Performance Testing of Response Capability

Response capabilities will nearly always be assessed as part of a whole system Security Assessment. However, given the potential importance of response elements in a security system, there is merit in designing performance testing for response elements on their own. Uniquely, these Security Assessments could be incorporated in a training especially where the response force has no other responsibilities. This can be readily achieved for a site response capability because it is usually subject to oversight by the regulatory authority and may be also under the control of the operator. However, off-site response is typically provided by local law enforcement and is not subject to oversight by the regulatory body. In these circumstances the operator should if possible include the need for Security Assessment in the formal arrangements for the response force.

### *Limited Scope Performance Test*

A limited scope performance tests provide an approach to evaluate the effectiveness of portions of the security system without conducting expensive and resource intensive force-on-force exercises. It can also be used to test system effectiveness of one or more elements of the system.

### *Force-on-force Exercises*

Force-on-force exercises allow the testing of the complete system, using the full features of the security system, to include the protective force. These activities are very resource intensive, requiring shadow forces, controllers, etc.

### **Performance Testing of security-related procedures carried out by personnel.**

The effectiveness of Procedural security measures can also be assessed independently of a whole system assessment. This might include checks on the effectiveness of two person rules, the effectiveness of searches etc. However this may more properly be seen as a training and refresher issue.

### **Uncertainties**

Assessment results will not be precise but have some uncertainties associated with them, given resource limitations on collecting required information described in section 4, limited precision about performance metrics such as delay times and detection probabilities derived from data libraries, imperfect knowledge about the precise status of the PPS and facility during an attack and the unpredictability about how adversaries or responders will react during an attack.

Uncertainties related to the variability that can be discerned from available data are frequently referred to as stochastic or aleatory uncertainties. These aleatory uncertainties are sometimes also referred to as irreducible uncertainties as an indicator that this type of uncertainty generally cannot be decreased. Aleatory uncertainties are accounted for during the assessment by allowing the variables related to detection, delay, and response to change over their range based upon a given model/distribution in the assessment data library. In general, the variables given in Table 1 are good examples of where aleatory uncertainties exist.

The area of uncertainty which relates to the shortcoming in analytical or experimentally based modeling is referred to as epistemic or modeling uncertainty. Partly due to the irreducible nature of the aleatory uncertainties, we tend to focus the understanding of uncertainty on these epistemic contributors. Such contributors may include uncertainty in the representation of the facility (e.g., the precise design of an ancient door may not be available), in the actual status of the PPS or how adversaries may respond to certain events or how responders may implement tactics. Therefore, the easiest way to identify epistemic uncertainties is to identify shortcomings and associated alternative models in for each of the four types of data described in the introduction to Section 4.

Table 4 identifies some significant sources of uncertainty in performing PPS assessments along with how these sources relate to the three data requirement categories.

Source	Data Requirement Category	Relationship to Human Performance	Description
1. Decision-making on responder deployment	Facility Characterization	This is directly related to human performance.	Details of how responders are deployed can be left to commanders and these commanders can make different decisions all within a given response plan. Given that the number of commanders is knowable, this uncertainty is really due to insufficient modeling.
2. Failure of security system components to function as designed	Facility Characterization	The failure (i.e., human error) of security forces (for whatever reason) is directly related to human performance.	Random failure of any system components (including officers). The failure modes for equipment components are generally knowable. This is not failure due to the adversary defeating the components (that failure is integral to the simulation), but rather an unrepaired/latent failure prior to attack.
3. Operating Modes	Facility Characterization	Not directly related to human performance	This is the uncertainty in the modeling of the defined operating modes (e.g., full power, refueling) of the facility. Some operating modes may occur only infrequently, but may represent increased vulnerability due to target set exposure or security design configuration. The number of operating modes is known so this uncertainty is due to insufficient modeling.
4. Environmental Conditions	Facility Characterization	Not directly related to human performance	This is uncertainty in the modeling of environmental conditions. Only choosing to model daytime and not nighttime operations is an example of this insufficient modeling uncertainty.
5. Weapon Performance (Ph Pk)	Performance Data Library	The hit and kill probability data attempts to remove any human performance bias.	Uncertainty in the current model of how weapons (both adversaries and security officers) perform. A ballistics-based model would likely reduce these uncertainties. Represents a needed research area since the current state-of-the-art is still using hit and kill probabilities.
6. Starting locations for adversaries and responders	Scenario Specific	Not directly related to human performance but is influenced by adversary and defender preferences.	Uncertainty of where adversary and defenders are located can affect planning assumptions set by attackers and defenders and their decisions during a simulation or exercise. The discrepancy between where these entities actually are versus where they are planned to be could affect the results of the analysis.

**Table 4.Sources of Uncertainty.**

Additional detail on developing data libraries is beyond the scope of this document.

## 2. Path Analysis

### *Introduction*

Path analysis looks at the options an adversary has to penetrate the various layers of a facility's security system. This may allow for multiple approaches for penetration of any given layer. The paths may be defined by a sequence of elements from an adversary sequence diagram or by a sequence of actions performed by an insider from an adversary action sequence diagram.

Path Analysis proceeds, in a general way, to determine measures of effectiveness of a physical protection system based on comparison of an adversary timeline and one or more response timelines.

...

It should be noted that in some cases different response forces may arrive at different times; in Figure E-2 forces show up at different times ( $T_1$ ,  $T_2$ ,  $T_3$ ); the forces that show up at each time are called contingents in this figure even if their arrivals at the same time are not coordinated. Three contingents are shown in Figure E-2, resulting in values  $PRT_1$  (which is the PRT shown),  $PRT_2$ , and  $PRT_3$ .

More generally, if there are  $K$  responding contingents, each sensing opportunity could have  $K$  possible different PRTs. The notation would be  $PRT_{jk}$  = the  $k$ th PPS Response Time associated with detection occurring due to sensing at sensing location  $j$ <sup>1</sup>.

...

Path analysis, then, includes searching over all paths looking for the one with the lowest  $P_1$ , etc. To find the best path, the other two issues need to be addressed. For example, some decision needs to be made about assigning detection and delay times based on all the different defeat methods that the adversary has at each step in the path. Finally, all facility states need to be addressed in some reasonable fashion. These issues will be discussed in Annex E.

### *Addressing Multiple Facility States and Targets*

An effectiveness evaluation may need to address effectiveness during each of several facility states, where the "state" refers to operational condition(s), weather condition(s), etc., and different targets. The combination of states and targets actually evaluated are determined by the analyst based on judgement about such factors as: how important the target is, how often the state occurs and whether its occurrence can be predicted, and whether physical protection for one facility state or target can be considered more effective than for another based on expert judgment.

---

<sup>1</sup> A more general model would define  $PRT_{jkn}$ , where  $n$  is a task on the adversary timeline. This case will not be covered here for a number of reasons but a remark will be made about this topic at the end of this section.



### 3. Scenario Analysis

Scenarios are hypothetical set of conditions and sequences of events constructed for the purpose of focusing attention on causal processes and decision-points. They answer two kinds of questions:

- Precisely how might some hypothetical situation come about, step by step?
- What alternatives exist for each actor, at each step, for preventing, diverting, or facilitating the process? (From Kahn and Wiener [1967], “The Year 2000, A Framework for Speculation”, ISAM definition)

Scenarios are commonly used to allow a range of possible future conditions and/or events to be modelled and assessed. A scenario may represent the conditions at a single point in time or a single event, or a time history of conditions and/or events (including processes). Safety analysts use accident scenarios to describe and model plant response to potential accidents. An accident scenario, which usually has an initiating event superimposed on a proposed plant configuration, can be used to model system response, including various operator actions as appropriate. (The definition from NSS. 4)

Nuclear security scenarios can be divided into several component stages, each addressing sub-objectives that the adversary has for that stage of the scenario; as examples, one can speak of a “pre-attack” or “planning” stage for a scenario before the adversary has attempted to penetrate a controlled or restricted area, or one can speak of the “transportation” stage of a scenario where material is being taken to some strategic location or major public event to be scattered or detonated. This document will refer to the scenario as that phase where a facility or transport operation is attacked by adversaries as opposed to the planning phase or what the adversary will do after the attack is successful.

Scenarios can be described as having attributes. Some examples of scenario attributes are the specific type of adversary involved, the target location, the use of special attack methods such as a cyber-attack, operating conditions, use of overt versus stealth, whether part of the attack is aimed at degrading the PPS through indirect attacks and whether an insider is used as part of the adversary’s hypothetical planning for or execution of the scenario.

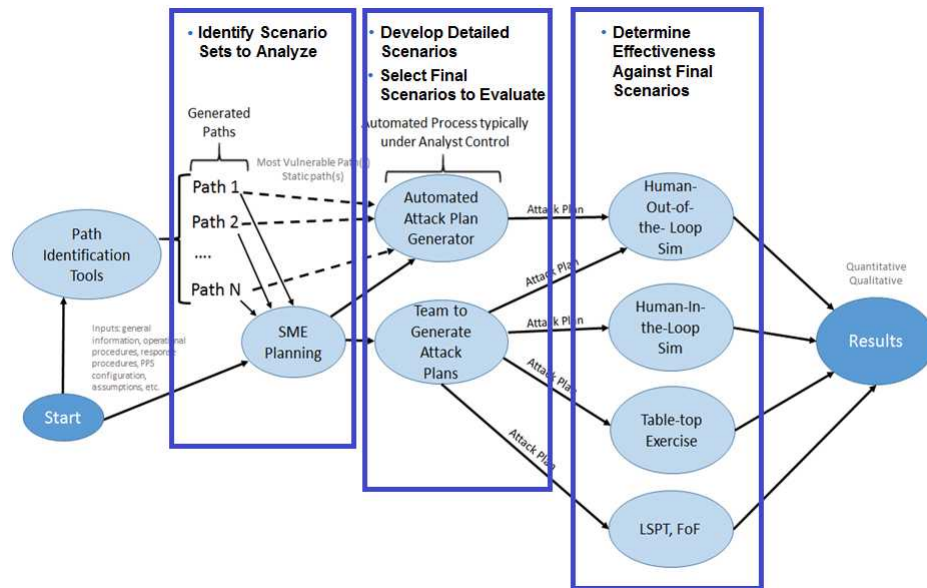
In turn, scenario classes can be defined in terms of scenario attributes, where each class conceptually includes all individual scenarios that have the corresponding scenario attributes. For example, scenario classes are commonly defined in terms of adversary objective (theft or sabotage), operational state(s) during which the attack occurs, the capabilities of the adversary and the adversary avenue of approach (e.g., from the sea versus land).

Scenario Analysis consists of four steps:

- Identify Scenario Sets to Analyze

- Develop Detailed Scenarios
- Review and Select Final Scenarios to Evaluate
- Determine Effectiveness Against Final Scenarios.

**Error! Reference source not found.** below shows how these steps line up with the process for using software tools and Evaluation Methods



**Figure 1. How Scenario Analysis Steps Correspond to the Process for Using Software Tools and Evaluation Methods**

### Identify Scenario Sets to Analyze

The first step in scenario analysis is to determine what set of scenario classes will be analyzed. A scenario class can be defined in terms of unique combinations of scenario attributes, where each class conceptually includes all individual scenarios that have the corresponding scenario attributes.

It is impractical to attempt to cover all scenario classes during the nuclear security assessment; hence it is important to plan what classes will be analyzed before starting to develop scenarios. In some cases, the competent authority or facility management may require that specific scenario classes will be addressed during scenario analysis; for example the competent authority may require that scenarios be developed for all buildings that contain Category I nuclear material. In other cases the assessment team will need to develop a planning document specifying which scenario classes will be evaluated.

For the purposes of this document the scenario set is an explicit or implicit list of all scenario classes that need to be analyzed. Table 1 shows a hypothetical scenario set based on selection of 4 scenario classes out of a total of 10 possible scenario classes.

	Objective: Unauthorized Removal of Category I NM	Objective: Sabotage
Operating Condition	Attack characteristics	Attack Characteristics
Operational Hours	#1 (land attack on foot)	Not evaluated
Off-Shift	Not evaluated	#2 (attack using a boat)
Inner Area In Use	#3 (land attack with vehicle)	Doesn't apply
Non-radiological emergency	Not evaluated	Not evaluated
Intra-site Transport	#4 (land attack on foot)	Doesn't apply

Table 1. Hypothetical Scenario Set to Be Evaluated

### Develop Detailed Scenarios

When developing attack scenarios, scenarios should be chosen to challenge the plant security and operations to the maximum extent practicable within the constraints established by a TA/DBT and the scenario class under consideration. Thus, the scenarios selected within each scenario class might be chosen as those for which the facility or transport is judged to be most vulnerable. As shown in **Error! Reference source not found.**, the scenario may be based on a most-vulnerable path generated by path analysis software or may developed by a team of experts. A process for scenario development is outlined below.

Detailed scenarios do not necessarily need to be developed for every scenario class in the scenario set. There may be very practical reasons why a scenario may make no sense to attempt, based on actual conditions. In other cases the analysis may run out of time or resources before all the scenario classes can be evaluated.

### Identify operational vulnerabilities

In order to identify site vulnerabilities across various operational conditions and states, consider different:

- Operational conditions (operational versus non-operational)
- Target material configurations (reactor load-out versus operations)
- Response force alert levels and personnel “crews”
- Different upgrade packages

### Exploiting the Vulnerabilities

When promising vulnerabilities have been identified, it will be required to develop an action plan how the each vulnerability will be exploited. The action plan will need to have the attention to detail

and organization in how the attack will be executed. The following steps can be followed (note that the scenario is hypothetical):

- First creating a list of essential tasks that have to be accomplished for the attack based on that vulnerability to succeed. Such a list might look like the following for a target:
  - Task 1: Enter building XYZ
  - Task 2: Collect 20 Kg of U235 in storage containers
  - Task 3: Leave site with material without pursuit by response forces
  - Task 4: Arrive undetected at safe house in city ABC
  - Task 5: Hold off responding units so that tasks 1 through 3 are accomplished

These tasks should be kept as simple as possible.

- Next, creating sub-plans that describe how one or more teams of attackers can perform each task within resource constraints. These sub-plans should describe:
  - Who is involved?
  - What are they doing as a function of time?
  - How are they performing each step?
  - What equipment are they using?
  - How are they transporting the equipment?
- Finally, combine these sub-plans into a master attack plan/scenario description, adjusting sub-plans to meet overall constraints imposed by the DBT and perhaps the site as well as to achieve synchronization between teams.

#### *Adding Supporting Team Sub-Plans to Scenarios*

Supporting teams can be assigned to complete other essential tasks or to aid the main team directly. Often, the remaining tasks look like: “Hold off responding units so ...” or “Neutralize offsite response...” Thus, one good use of supporting teams is to delay or incapacitate the response through setting ambushes, creating diversions, and attempting to confuse the response.

#### *Using Path Analysis for Scenario Development*

Path analysis can suggest sub-plans that serve as the main or “direct” part of the attack (direct in the sense of going to the target). Such plans might be based on the minimum delay, minimum  $P_I$ , or minimum  $P_I * P_N$  paths

Details can be added to these path descriptions to fill out the scenario. For example, instead of the step “Penetrate Fence” found in the path analysis, the scenario description might consist of: “Four adversaries bridge fence using ladder carried in from vehicle parked outside at night during a storm. Last adversary monitors radio traffic.”

Of course, multiple scenarios can be developed for a single path by slightly varying the method by which the adversary attacks different protection elements along the path.

Be aware, though, the most-vulnerable path (MVP) from path analysis may be a poor basis for creating a scenario. This may occur because typically low  $P_1$  paths should be corrected with upgrades during the path analysis phase. After such upgrades, the MVP should now have a high  $P_1$  rendering that path less desirable. At this stage scenario analysis might more profitably consider factors not found in path analysis: preventing neutralization and employing other teams to prevent interruption.

### **Review and Select Final Scenarios to Evaluate**

Either while the scenario are being developed or at the end of that process, the scenarios need to be reviewed to determine what scenarios will be evaluated or not. This review and selection may involve stakeholders, such as staff from the competent authority or facility management. Written scoping agreements may be created to document assumptions about which scenarios to evaluate or what set of evaluation tools will be used and in what order, etc.

Part of this review should consider whether all of the objectives for the current assessment have been covered by the set of scenarios selected. Another consideration is whether all of the scenarios selected appear to be credible and within the capabilities specified in the TA/DBT. If there are issues with either of these concerns then the assessment team may need to revise some of the existing scenarios or develop new ones.

### **Determine Effectiveness against Scenarios**

Figure 1 shows 4 types of evaluation tools/methods that can be used singly or in combinations to evaluate scenarios: Human-in-the-Loop Combat Simulations, Human-out-of-the-Loop Combat Simulations, Tabletop Exercises, and LSPT/FoF Exercises. The choice of which combination to use will depend upon a number of factors, such as the nature and size of the facility, the type of assessment and its objectives. In some instances it may be sufficient to conduct a table-top exercise.

#### ***Simple Timeline Approach***

This approach assesses the detection and delay elements of the scenario to determine whether the response force can interdict the adversary force. Note: it may turn out that a simple calculation shows the response cannot arrive in time so that further detailed scenario simulation/exercises (as described below) are unnecessary.

### *Table-top Analysis*

This tool can be used for a couple of purposes. It can be used to assess the security system effectiveness along a given scenario, using expert input. It can also be used to help response organizations better understand how to interact and achieve success in defeating the adversary.

### *Computer Simulation*

Computer models and simulations still require extensive input and may require several people to play roles in the conflict analysis. It should be noted that the quality of computer tools in general tend to be limited by the quality of the data included with the simulation software. Computer simulation requires very detailed description on scenarios such as an attack plan.

### *Force-on-force analysis*

Force-on-force analysis allows the testing of the complete system, using the full features of the security system, to include the protective force. These activities are very resource intensive, requiring shadow forces, controllers, etc. Because a FoF is resource intensive and contain some artificiality such as assumed weapons effects or safety constraints, an alternative is to conduct a combination of limited scope performance testing, tabletops, or computer modeling/simulation in lieu of full FOF exercises. It's a good idea to compare FOF exercises with assessment analysis results for comparison of data.

More information about FoF exercises is provided in X.

### **Combinations of Nuclear Security Methods and Tools Suggested for Different Conditions**

The following two tables suggest combinations of assessment methods and tools that might be useful for different types of facilities and during different stages in the facility lifecycle. For example, Table 2 indicates that computer simulations and path analysis are probably not appropriate for evaluating a Spent-Fuel Storage facility.

Careful planning should be performed before every evaluation to select the best set of methods and tools to use during that evaluation. In particular, the methods and tools to use may be dependent on the states regulatory requirements for graded protection and details about the TA/DBT.

	Assessment Methods and Tools to Use for Different Target Facilities/Activities				
Methods and Tools	NPP/Cat I Facilities	Irradiator Facility	Transport	LEU Fuel Fabrication	Spent-Fuel Storage
Checklist	X	X	X	X	X
Sampling	X	X	X	X	X
Observation	X	X	X	X	X
Table-tops	X	X	X	X	X
Computer Simulations	Optional		Optional		
Path analysis	X	X	X*	Optional	
Performance Testing	X	X	X	X	X
Response Force Tests	X (includes Force-on-Force)	Optional	X (includes Force-on-Force)	Optional	X

**Table 2. Hypothetical Combinations of Methods and Tools Appropriate for Different Types of Nuclear Facilities**

\*-Would apply when transport is at a Safe Haven

Methods and Tools*	Siting	Design	Operation	Decommissioning	Post-Closure
Checklist	X	X	X	X	X
Sampling			X	X	X
Observation			X		
Table-tops		X	X	X	
Computer Simulations		X	X		
Path analysis	Very simple	X	X		
Performance Testing			X	X	
Force-on-force exercise			X		

**Table 3. Nuclear Security Assessments Appropriate For Different Facility Lifecycle Stages**

**The following should go to an Annex; I am not sure which one.**

### **X: Conducting A Force-on-Force Exercise**

(This needs to be moved to an Annex on Force-on-Force)

In a force-on-force exercise the security assessment project team should be installed in a location where they are equipped to receive updates from all participating teams and observers, and with the ability to communicate with the Control Rooms around the facility; process, security and emergency.

Other than being aware that they are participating in an exercise, not a real incident, all participants should have no prior knowledge of the scenario. They should not be aware of the initiating incident, the target(s), or the nature of the threat. The affected facility staff should know that it is a force-on-force exercise that is being undertaken. Those facility staff should be aware of the expected duration of the exercise, as is also true for the 'players' in the scenario(s).

In all respects other than these, participants should either, carry on with their duties as they would normally be expected to do or, carry out their instructions as to what to do in an incident.

Observers, clearly identifiable as such, should be present in all parts of the exercise including, periodically, to check on the well-being and understanding of non-exercise participants. If, for example, the scenario requires the use of explosives in a location, an explosive, of course, should not be used but the Observer will rule if the explosive has been deployed and to what effect.

The end of the exercise should be signaled by the Project Manager according to criteria agreed in advance. All participants, and all who have been inadvertently swept up in the exercise, should be debriefed as soon as possible. The latter group's debriefings can usually be short but they should be asked if they have any observations to make on ways in which security and response might be improved. It is imperative that concern is shown for their welfare, and appropriate support is available if necessary. Even though it has been an exercise that has been deprived of control over their lives and some will have been traumatized. Active participants should be debriefed more thoroughly to ascertain the effectiveness of the scenario and exercise control systems, the effectiveness of the security processes, and any other observations they may have.

Special consideration needs to be given to the use of armed response. States have different laws and social expectations. In general, it is not necessary to deploy arms in such an exercise. It should be sufficient for the Observers to judge whether or not sufficient has been done to disable the adversary. Response forces may feel that their skills have not been tested but it needs to be emphasized that this is not a training exercise, and this is a test of system performance.